CLAIMS

1. A method for de-authenticating a client device from a network based on a credit based access control, said method comprising:

receiving, by an access point (AP), in the network a user request for user access from said client device according to an authentication protocol;

transmitting, by said AP, an access request to an authentication server in response to said user request;

receiving, by said AP, an access response from said authentication server authenticating said user access for said client device, the access response containing a parameter having a credit value indicative of a length of available continued access of the client device to the network based on remaining user credit;

transmitting, by said AP, a first re-authorization request to said client device in response to said credit parameter value reaching a threshold value to cause a re-authentication of said client device with said network to occur;

receiving, by said AP, a first re-authorization response from said client device, in response to said first re-authorization request; and

transmitting a second re-authentication request to said authentication server before granting further access to the network by said client device.

2. The method of claim 1, wherein said parameter comprises a session-timeout parameter associated with IEEE 802.1X authentication protocol.

3. The method of claim 1, further comprising transmitting by said authentication server, in response to said second re-authentication request from the AP, a second re-authentication response for re-establishing access to said network based on said credit parameter value associated with the client device on said authentication server.

4. The method of claim 3, wherein the second re-authentication response is one of a a) de-authentication message; and b) re-authentication message, based on the results of a comparison of said credit parameter value with said threshold value by said authorization server.

5. The method of claim 1, wherein said credit parameter value contained in said access response is based on one of: a) time usage; and b) traffic volume usage.

6. The method according to claim 1, wherein said network is a wireless Local Area network (WLAN) and further wherein said client device is a mobile communications device.

7. A method for de-authenticating a client device from a network based on a credit based access control comprising the steps of:

receiving, by an authentication server, an access request for access to said network by said client device according to an authentication protocol;

providing, by said authentication server, an access response to an access point (AP) of the network authenticating the client device, the access response containing a parameter having a credit value indicative of the length of available continued access of the client device to the network based an indicator of remaining user credit, so as to cause a re-authentication of the client device to occur in the event said credit parameter value reaches a predetermined threshold value.

8. The method of claim 7, further comprising calculating by said authentication server said credit parameter value based on said indicator of remaining user credit and network charges.

9. The method of claim 7, wherein said parameter comprises a session-timeout parameter associated with IEEE 802.1X authentication protocol.

10. The method of claim 7, further comprising, in response to a re-authentication request from said AP associated with said client device, said authentication server compares said credit parameter value for the associated client device, with said predetermined threshold value and transmits a de-authentication response message to the AP when the value of said credit parameter value reaches said predetermined threshold value.

11. The method of claim 7, wherein said authentication server comprises a RADIUS server operating IEEE 802.1X authentication protocol, and further comprising storing in said authentication server said credit parameter value associated with a user of said client device for accessing said network, and updating said credit parameter value according to one of: a) time usage; and b) traffic volume usage and further wherein said network is a wireless Local Area Network (WLAN) and said client device is a mobile communications device.

12. A network comprising:

an access point for communicating with one of a plurality of client devices through a communications channel, said access point providing access to said network based on an authentication of said client device via an authentication server according to an authentication protocol,

wherein said access point is further responsive to an access response from an authentication server authenticating one of said client devices having requested access to said network, which request was forwarded to said authentication server via said access point, said access response containing a parameter having a value indicative of the length of available continued access of the client device based on an indicator of remaining user credit, so as to cause said access point to initiate a re-authentication process upon the expiration of a time period corresponding to said parameter value, thereby requiring re-authentication of the client device before granting the client device further access to the network.

13. The network of claim 12, wherein the network operates using an 802.1X authentication protocol, and wherein the authentication server is a RADIUS authentication server and further wherein said network is a wireless Local Area Network (WLAN) and said client device is a mobile communications device.

14. The network of claim 12, wherein said parameter value comprises a session-timeout parameter.

15. The network of claim 13, wherein said RADIUS authentication server contains memory for storing said indicator of remaining user credit.

16. The network of claim 12, wherein said parameter value contained in said access response is based on one of: a) time usage; and b) traffic volume usage.

17. The network of claim 15, wherein in response to a re-authentication request associated with the client device received from the AP, the authentication server retrieves said indicator of remaining user credit and denies re-authentication of said client device when said indicator of remaining user credit drops below a threshold value.

18. The network of claim 17, wherein the indicator of remaining user credit comprises a credit timer indicative of the remaining credit balance of said user account, said credit timer being decremented according to a temporal access usage to the network by the client device.

19. The network of claim 17, wherein the authentication server periodically updates the credit timer of said user account in units of: a) time and b) traffic volume.

20. A method for de-authenticating a client device from a network based on a credit based access control, said method comprising:

receiving, by an access point (AP), in the network a user request for user access from a client device according to an authentication protocol;

transmitting, by said AP, an access request to an authentication server in response to said user request;

calculating, by said authentication server in response to said access request, a session-timeout parameter value based on remaining user credit and network charges associated with said client device, said session-timeout parameter value indicative of the length of available continued access to the network;

embedding, by said authentication server, said session-timeout parameter value in an access response message authenticating said associated client device for network access and transmitting said access response message to said AP;

activating, by said authentication server, a credit timer having a value indicative of remaining user credit balance associated with said client device, said credit timer decremented according to a temporal access usage;

receiving, by said AP, said transmitted access response message and granting access to the network by the associated client device;

determining, by said AP, when the session-timeout parameter value expires;

transmitting, by said AP, a first re-authorization request to said client device in response to said session-timeout parameter value expiring;

receiving, by said AP, a re-authorization response from said client device in response to said first re-authorization request

transmitting a second re-authentication request to the authorization server in response to said re-authorization response;

receiving by said authentication server said second re-authentication request for re-authenticating said user access for said associated client device, comparing said credit timer value associated with said client device with a predetermined threshold value, and determining whether said client device is de-authenticated from further access to the network based on said comparison.

21. The method of claim 20, further comprising transmitting by said authentication server a de-authentication response message to said AP when said credit timer value is below said predetermined threshold value.

22. The method according to claim 20, wherein said network is a wireless Local Area Network (WLAN) and said client device is a mobile communications device.

23. A network for de-authenticating a client device from said network based on a credit based access control comprising:

means for receiving, by an access point (AP), in the network a user request for user access from a client device according to an authentication protocol;

means for transmitting, by said AP, an access request to an authentication server in response to said user request;

means for receiving, by said AP, an access response from said authentication server authenticating said user access for said client device, the access response containing a parameter having a value indicative of the length of available continued access of the client device to the network based on remaining user credit;

means for transmitting, by said AP, a first re-authorization request to said client device in response to said parameter value reaching a threshold value to cause re-authorization of said client device with said network to occur;

means for receiving , by said AP, a re-authorization response from said client device in response to said first re-authorization request; and

means for transmitting a second re-authentication request to said authentication server before granting further access to the network by said client device.

24. The network according to claim 23, further wherein said network is a wireless Local Area Network (WLAN) and said client device is a mobile communications device.

25. A method for de-authenticating a client device from a network based on a credit based access control, said method comprising:

receiving, by an access point (AP), an access response from an authentication server authenticating user access for said client device, the access response containing a parameter indicative of an amount of available access of the client device to the network based on remaining user credit;

determining a remaining amount of available access of the client device in response to usage of the network by the client device and parameter;

transmitting, by said AP, a first re-authorization request to said client device in response to said remaining amount of available access reaching a threshold value to cause a re-authentication of said client device with said network to occur;

receiving, by said AP, a first re-authorization response from said client device, in response to said first re-authorization request; and

transmitting a second re-authentication request to said authentication server before granting further access to the network by said client device.

26. The method of claim 25, wherein said parameter comprises a session-timeout parameter associated with IEEE 802.1X authentication protocol.

27. The method of claim 25, further comprising transmitting by said authentication server, in response to said second re-authentication request from the AP, a second re-

authentication response for re-establishing access to said network based on said credit parameter value associated with the client device on said authentication server.

28. The method of claim 27, wherein the second re-authentication response is one of a a) de-authentication message; and b) re-authentication message, based on the results of a comparison of said credit parameter value with said threshold value by said authorization server.

29. The method of claim 25, wherein said credit parameter value contained in said access response is based on one of: a) time usage; and b) traffic volume usage.

30. The method according to claim 25, wherein said network is a wireless Local Area network (WLAN) and further wherein said client device is a mobile communications device.